Anno 3 - N. 43
29 Gennaio 2004 - 12 Febbraio 2004

Direttore Responsabile: Luca Sprea

I Ragazzi della redazione europea:
grand@hackerjournal.it, Il Coccia, Gualtiero Bismark.it, Tronconi, Ana Esteban, Marco Bianchi, Edoardo Bracaglia, One4Bus, Barg the Gnoll, Amedeu Bruguès, Gregory Peron

Service: Cometa s.a.s.

DTP: Davide Colombo

Graphic designer: Dopla Graphic S.r.l.
info@dopla.com

Copertina: Davide Fo e Il Coccia

Publishing company
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing
Roto 2000

Distributore
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81-
Tel. 06.33455.1 r.a.
20134 Milano, V.le Forlanini, 23
Tel. 02.75417.1 r.a.

Abbonamenti
Staff S.r.l.
Via Bodoni, 24
20090 Buccinasco (MI)
Tel. 02.45.70.24.15
Fax 02.45.70.24.34
Lun. - Ven. 9,30/12,30 - 14,30/17,30
abbonamenti@staffonline.biz

Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

HJ: INTASATE LE NOSTRE CASELLE

Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati. **redazione@hackerjournal.it**

hack·er (hãk'∂r)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

COLPA LORO

Art. 615-quater. Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino a un anno e con la multa sino a lire 10 milioni.

La pena è della reclusione da uno a due anni e della multa da lire 10 milioni a 20 milioni se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'art. 617-quater.

Legge 23 dicembre 1993 n. 547 (G. U. n. 305 del 30 dicembre 1993) - Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica

Il testo qui sopra si può recuperare, tanto per dirne uno, a http://www.interlex.it/testi/l547_93.htm. Al solito, in Italia, le leggi non sono fatte per fare vivere in pace le persone normali e per punire i criminali, ma all'insegna della peggiore FUD: Fear, Uncertainty, Doubt, paura, incertezza, dubbio. Le armi con cui si mantiene il potere quando si sa di non avere ragione. O forse, in questo caso, quando non si sa di che cosa si stia parlando.

Che cosa vuol dire procurare un profitto? Se un hacker scopre qualcosa che non va nella rete di sicurezza di un'azienda non ne può parlare su una rivista (dopo avere avvisato l'azienda) perché la rivista si vende in edicola e quindi l'editore ne ricava un guadagno? Quali sono le misure di sicurezza che proteggono un sistema informatico o telematico? Vuol dire che se un criminale ruba una password a uno sprovveduto che non ha protetto il proprio sistema la passa liscia? Se un disonesto incontra un imbecille in fiera, attacca bottone e si fa dire – chiacchierando come tra amiconi – qual è la password che spalanca le porte di una rete, si è procurato una password abusivamente? E se un deficiente con uno script in mano distrugge un sistema senza trarne profitto, per il gusto semplice e stupido di farlo, ha violato la legge o no?

Non diteci che il comma questo o l'articolo questo rispondono alle nostre domande. Scommettiamo che, codice penale alla mano, si trova in breve una falla che consente di commettere un crimine informatico e farla franca?

Questo è il Paese dove, anticamente, non si poteva tenere un modem in casa se non era un modem SIP e dove, per poter fare una chiamata via modem, bisognava pagare una tassa di concessione per utenza telegrafica. Guai a chi pensava di poter trasmettere dati senza essere omologato, in tutti i sensi.

È il Paese dove possiamo pubblicare, in questo numero, un articolo che interessa sessanta milioni di persone, ma che dobbiamo soppesare parola per parola, plotone di avvocati alle nostre spalle, perché il confine tra la libertà di informazione tecnica e la galera è quanto mai sottile.

Se trovate che manca un pezzo, o che qualcosa non è chiaro, non prendetevela con noi. Prendetevela con Loro. C'è gente che non vuole che le cose si sappiano.

Comunque buona lettura. E sotto con l'hacking!

Barg the Gnoll
gnoll@hackerjournal.it

One4Bus
one4bus@hackerjournal.it

FREE HACK NET

Saremo di nuovo in edicola Giovedì 12 Febbraio !

La prima rivista hacking italiana

Bufala fresca

Unite Power Point a un mago da quattro soldi e otterrete una super-bufala, che di fresco ha solo le lacrime al pensiero che qualcuno ci caschi.

Sta diffondendosi a macchia d'olio ed è l'ennesima email che cercherà di terrorizzarvi facendovi credere che se non aderirete alle proposte del mago "David Copperfield", una perfida maledizione vi inseguirà per il resto dei vostri giorni. Si tratta di email con allegata una presentazione .pps

Dopo un po' di suspance (vi è concesso qualche sbadiglio soprattutto se non siete dei fans di Power Point…) vi verranno mostrate 6 carte diverse. Il giochino proposto vuole far credere che il ciarlatano di turno indovinerà la carta che avete pensato (solo pensato, senza clic!), leggendovi nella mente attraverso lo schermo (sic!). La videata successiva vi mostrerà infatti cinque carte, tra le quali quella pensata… _NON_ compare. Come ha fatto? Un suggerimento: ma ve le ricordate tutte le carte che avete visto?

Prima, durante e dopo

Mauro ci invia l'immagine con un solo commento: "Volevo Inviarmi Un Immagine Di Mia Creazione"

Eccola pubblicata. Certo, 700 MB di regali potrebbero viziare chiunque… Coraggio, un po' di esercizio ancora e potresti avere davanti a te una carriera di copy. Un domani ;)

Nuova password!

Ecco i codici per accedere alla Secret Zone del nostro sito, dove troverete gli arretrati, informazioni e approfondimenti interessanti. Con alcuni browser, potrebbe capitare di dover inserire due volte gli stessi codici. Non fermatevi al primo tentativo!

user: bresil

pass: colombia

SECRETZONE

Un altro PUNTO di riferimento

Volevo segnalare il sito della mia crew... ci stiamo dando da fare affinchè diventi "qualcosa di grosso" un punto di riferimento per la rete... (lo so siamo megalomani) il link è www.hackerlaws.tk z3ro

Bello! Dobbiamo decisamente complimentarci anche per la grafica adottata. Visitabile, consigliabile. Auguri di crescita anche a voi!

Sotto con gli overclokkati

Salve a tutta la redazione di HJ, volevamo segnalarvi il nuovo portale informatico che abbiamo creato... http://www.overclokkati.com/
FrancescoFra & PuMaX

Un po' scarno, al momento della pubblicazione, ma crescerà! Bravi!

mailto:
redazione@hackerjournal.it

SOCIAL ENGINEERING PRO VIRUS

Salve, sono un ragazzo di 17 anni;
ieri mentre leggevo la posta mi sono accorto di una strana e-mail, vi riporto qui sotto il contenuto: (vedi sotto)
In allegato a questa e-mail c'era un file txt chiamato: Norton AntiVirus eliminato1.txt, che conteneva queste due righe: Norton AntiVirus ha rimosso l'allegato: refcode10214.txt.pif. L'allegato era infettato con il virus W32.Sober.C@mm.
Volevo sapere se è veramente un'e-mail dell'fbi o se è solo qualcuno che non ha di meglio da fare che rompere. Grazie per la cortese attenzione. La vostra rivista è mitica

Alessandro

Gentile redazione,
tralascio i meritatissimi complimenti per la vostra rivista che leggo dal numero 2. Ho ricevuto il 1° gennaio una mail anomala che apparentemente arriverebbe dal mio stesso indirizzo, ma che ovviamente non mi sono mai autoinviato.
La mail in questione aveva come oggetto: "Your IP was logged" ed anche un allegato con una doppia estensione (refcode17559.txt.pif) che mi ha insospettito, ma che la scansione in linea di yahoo mail effettuata con Norton Antivirus non ha riscontrato come infetto.
Avete dei consigli o delle delucidazioni da darmi in merito?

Andrea

Ladies and Gentlemen,
Downloading of Movies, MP3s and Software is illegal and punishable by law.

We hereby inform you that your computer was scanned under the IP 172.189.72.58 . The contents of your computer were confiscated as an evidence, and you will be indicated. In the next days, you\'ll get the charge in writing. In the Reference code: #10214, are all files, that we found on your computer.

The sender address of this mail was masked, to protect us against mail bombs.

- You get more detailed information by the Federal Bureau of Investigation -FBI-
- Department for \"Illegal Internet Downloads\", Room 7350
- 935 Pennsylvania Avenue
- Washington, DC 20535, USA
- (202) 324-3000

Cari Alessandro e Andrea,
beh, la seconda ipotesi è quella giusta... c'è sempre in giro qualcuno che ha voglia di rompere le scatole agli altri e non ha di meglio da fare che inventarsi nuovi modi per diffondere virus.
E che dimostra quanto siamo portati a credere alle favole, purché dette bene da qualcuno di più autorevole :-(

Provate a leggere il documento a questo indirizzo: http://attivissimo.homelinux.net/security/soceng/soceng.htm e avrai conferme di quello che stiamo dicendo, che fa parte del social engineering, usato per barare.
Quanto agli antivirus: beh, raga, qui ci vuole un antivirus con le palle e soprattutto aggiornato costantemente. Se non becca un virus così, c'è da cominciare a sudare freddo...

PARLI COME BADI!

Ciao. Mi chiamo Luca e passo subito al "sodo";
ho notato che molti, come me, hanno difficoltà nello svincolarsi fra i vostri articoli. E' oltremodo frustrante impantanarsi nella lettura di un argomento che ti appassiona, perchè non conosci il significato di alcuni termini o concetti. Non si tratta altresì di parole di uso comune, facilmente reperibili su un dizionario! Ho comunque notato che ultimamente tendete a specificare sempre più anche quelle cose che per un "ossessionato" sono addirittura banali e scontate. E fate bene. Basta mettere fra parentesi un paio di parole "umane" per spiegare cose altrimenti incomprensibili. Vi consiglio di implementare sempre più questo modus operandi, poiché renderà più piacevole la lettura anche ai non espertissimi come me (oltre ad aiutarci a diventarlo!).
Vorrei lanciare un messaggio a tutti coloro i quali ritengano "palloso" leggere articoli pieni di cose per loro scontate: "nessuno è nato studiato" e quel che sapete lo sapete perchè avete avuto il tempo, la voglia e la costanza di impararlo, ma anche la fortuna di poter attingere alle fonti giuste!! Nessuno impara veramente da solo.

Luca

Ciao Luca.
Difficile dare il giusto equilibrio e accontentare tutti, vero? Ma in fondo una cosa sola ci interessa: dare lo spunto per far partire lo spirito giusto. È come quando si fa un viaggio all'estero: magari non so bene la lingua, forse non conosco le abitudini del luogo dove mi sto recando, certamente farò delle figuracce in chissà quante occasioni. E allora i casi sono due: o non parto più, o parto cogliendo tutto come un'occasione unica per aprire la mente e gli occhi, imparare cose nuove, magari anche capire che non sono solo a trovarmi in situazioni analoghe e cominciare a parlarne!
Nessuno nasce imparato, diceva Antonio de Curtis, in arte Totò (approposito, anche il titolo è suo: ma lo sapevi, vero?!). E la grande curiosità, è l'unica medicina e lo spirito del vero hacker.
Sei ancora in ascolto? E allora divertiti con http://www.antoniodecurtis.com/

MONITOR E FOTO

Quando i monitor dei PC si vedono in TV ci sono sempre delle barre che scorrono dall'alto verso il basso.
Dopo lunga meditazione ho concluso che questo effetto viene creato dalla diversa velocità di refresh dello schermo PC rispetto alla velocità dei singoli fotogrammi.
Essendo i fotogrammi + lenti del refresh del monitor non riescono a filmare l'intera sequenza ed è per questo che l'immagine risulta a scatti. Aspetto smentite. A presto

Giaipur

www.hackerjournal.it

Caro Giaipur,
complimenti per le tue deduzioni.
È un po' quello che accade anche quando si cerca di fotografare uno schermo TV. Ma vediamo allora come si fa a fare una bella fotografia senza i problemi di barre indesiderate.
Innanzitutto disattivate il flash, non serve e darebbe un sacco di problemi. Poi impostate una sensibilità minima, diciamo 100 ASA. Mettete il tutto su cavalletto o su un altro supporto che vi permetta di centrare esattamente l'obiettivo con lo schermo.
Se vi posizionate un po' distanti e usate lo zoom, verrà ancora meglio perché si evitano le linee storte.
Meglio anche oscurare tutto, eliminare le eventuali luci e coprire i LED dei televisori. Il buio, insomma, evita di vedere strani riflessi colorati. Il tempo di esposizione deve essere uguale o più lungo del tempo di tracciamento dell'immagine sullo schermo, altrimenti verrà fuori il problema che dice il nostro Giaipur: non viene riprodotta l'immagine intera. Nel caso di un TV, un fotogramma viene disegnato in 1/25 di secondo. Se il tempo di scatto è inferiore, il risultato sarà una foto incompleta o con le bande. I migliori risultati in genere si ottengono con tempi di 1/4 o 1/8 di secondo. Con le animazioni o con i film è necessario però impostare un tempo di esposizione pari alla frequenza di refresh utilizzata. Mettete a fuoco se già non avviene automaticamente e zac! ci siete.
Un'ultima curiosità: perché adottare questa tecnica anche ai monitor PC, quando esistono i salvaschermo? Perché spesso i salvaschermo non riescono a catturare immagini provenienti in diretta (tramite streaming) dai siti 'live'. Per non trovarvi un blocco nero o violaceo, l'unica soluzione è usare la macchina fotografica.

C'È ANCORA CHI CI CREDE?

Dalla posta mi arriva regolarmente una patch, che dal mittente risulterebbe "Microsoft". Dato che uso Linux la patch non mi serve, né la voglio, ma anche le mie proteste in risposta non servono a niente. […] Mi domando se questo messaggio sia veramente una sorta di virus della Microsoft o se sia solamente un virus mandato da chissachi.
Vi mando la pach da controllare (ovviamente non apritela senza le dovute precauzioni.... :-). Distinti saluti.

Roberto

"From: "Microsoft" <security@microsoft.com>
To:
Dear friend , use this Internet Explorer patch now!
There are dangerous virus in the Internet now!
More than 500.000 already infected!

patch.exe"

Gentile Roberto,
hai pensato bene di non aprire la patch, ma ancora meglio avresti fatto non rispondendo a nessun messaggio del genere. Pensaci un po': ti pare che Microsoft, per quanto tu sia un accanito sostenitore di Linux, mandi in giro dei messaggi email con gli aggiornamenti del software? Semmai, come fanno tutte le grandi organizzazioni, attiva un sito da cui scaricare in modo controllato e sicuro tutto quello che potrebbe servirti. Per di più rispondere a tutte quelle email che ti dicono qualcosa come "se non vuoi ricevermi più, clicca qui", è come dire a chi ti manda spam "eccomi, esisto e sono attivo. Per favore, riempimi di spam tue e di tutti quelli a cui hai venduto (a caro prezzo) il mio indirizzo. Per di più tra quelli che valgono, perché funzionanti!"
Quindi: buttare subito tutto quello che non sapete da dove vi arrivi e del perché vi sia stato inviato. È l'unico modo per evitare pasticci. Poi attivare un buon antivirus tenuto _sempre_ aggiornato (tranquillo, il tuo file allegato è stato eliminato in modo automatico dal nostro antivirus) e usare, con parsimonia, le opzioni antispam del provider. Ecco fatto, non ci caschi più :-)

TROVAMI LA EX

Ciao ragazzi, è inutile dirvi ke siete davvero forti ;) Vi scrivo x un prob ke ho. Ho letto l'articolo sul n°40 "stringere il cerchio". Era da ytempo che cercavo degli url x trovare xsone che non sai + come e dove trovarle sul web. Ho provato tutti gli url pubblicati ma non sono riuscito a trovare la xsona ke vorrei cercare. Premetto: questa xsona è una xsona che è stata da prima la mia migliore amica e poi la mia ragazza. purtroppo ha una brutta malattia e non so se ce la farà......... io vi dgt da napoli lei è napoletana e si trasferì a rimini. Da allora non ho avuto + sue notizie. vorrei tanto rintracciarla ma non so come fare. potete aiutarmi x favoreeeeeee vorrei saxe come sta, cosa sta facendo.. insomma avete capito no?!!! se decidete di aiutarmi in questa impresa ve ne sarò grato x sempre.... mandatemi un risposta e io vi darò i suoi dati ke ho a disposizione.
grazie 1000, auguri e in culo alla balena x la vostra rivista strafica!!!

.::Momix::.

Ciao a te .::Momix::.!
Grazie dei compli, ecc ecc. Ti diciamo nell'orecchio una cosa: anche "stringere il cerchio" è nato da una esperienza più o meno come la tua! Il primo amore non si scorda mai: vero! Vabbé, ma allora come fare? Certamente cercare i privati è maledettamente difficile. E meno male. Pensa sennò quanti rompi avresti tra i c… anche tu! Però, però… se uno ci tiene sul serio si muove e non si dà pace. E allora, forse, ci riesce. Forse spendendoci qualche soldino, a volte anche no. Ti spiego. Forse non sai che i Comuni (si, quelli col sindaco dentro…) hanno le cosiddette liste elettorali. E forse non sai che sono a disposizione di chiunque ne faccia una richiesta per uno scopo ragionevolmente credibile: chessò, offrire posto di lavoro ai diciannovenni appena diplomati. A volte chiedono qualche soldo (una ventina di Euro, al più). A volte non chiedono nulla se non di firmare un foglietto che ti spediscono .pdf, in cui si dichiara che non verranno usati per scopi illeciti. E lì trovi tutta l'anagrafica comunale dai diciott'anni in su, ovviamente senza numero di telefono. Ma non dirmi che, rileggendo l'articolo, non saresti in grado di arrivare a un numero di telefono a partire da un nome e indirizzo…
E come fare a contattare i Comuni? Niente di più semplice: www.comuni.it. Indirizza le tue richieste a Ufficio Elettorale, ma mi raccomando: non dire che ti abbiamo mandato noi! :-) E dai che la trovi!

NEWS

HOT!

UN GIUDICE SENZA PARAOCCHI

Il Tribunale di Bolzano ha riconosciuto un diritto sacrosanto. Una recente sentenza reperibile anche su www.ict-law.net, infatti, afferma che i mod-chip di modifica della Playstation non sono illegali perché consentono:
- di superare ostacoli monopolistici
- di leggere dischi di importazione (e ciò potrà non fare piacere ai distributori europei, ma non viola alcun diritto d'autore)
- di leggere dischi prodotti da società diverse da quella che ha prodotto la Playstation
- di leggere la copia di sicurezza del software che la legge italiana consente di procurarsi
- di leggere supporti di contenuto diverso da quello originariamente previsto, ma legali;
- di sfruttare tutte le capacità della Playstation come computer.

"Vediamo infine se il produttore della macchina possa vietarne un uso diverso da quello da lui voluto.
In base alle nostre norme civilistiche, la risposta è senz'altro negativa: chi è proprietario di un bene può goderne nel modo più ampio ed esclusivo"

Finalmente! Grazie, signor Giudice.

OKKIO ALLE MAIL DI CITIBANK

È in atto una truffa attraverso l'invio di email a nome Citybank che invitano i destinatari a fornire i propri dati. Lo stratagemma utilizzato è quello di richiedere una verifica del proprio account con relativa immissione dei propri dati. L'e-mail risulta proveniente dalla banca, che in realtà non ha niente a che fare con il sito in questione. Maggiori info le trovate al sito:
http://www.citibank.com/italy/homepage/

BALLE ADSL: SOLO FASTWEB NON TRADISCE

Ve la fanno aspettare, è vero. Ma è altrettanto vero che in quanto a velocità la linea ADSL di Fastweb è un vero sballo! Vi dicono tutti che la velocità delle linee ADSL non è mai quella dichiarata. Nel caso di Fastweb non è vero: 2 Mbps sono due mega bit per secondo, sempre, a vostra totale disposizione. E anche in upload si viaggia a mezzo Mega, sempre, con sicurezza. Veramente eccezionale, per chi ancora non riesce a essere raggiunto dalla fibra. Fate la prova voi stessi, utilizzando uno dei servizi di controllo della velocità di connessione, come http://us.mcafee.com/root/speedometer.asp

ADRIAN LAMO HA SEMPRE PIÙ PAURA...

Dopo essersi costituito all'FBI alcuni mesi fa, Adrian ha espresso il proprio pentimento, dicendosi pronto a rispondere delle famose intrusioni di cui è stato protagonista. (http://adrian.adrian.org)
Adrian Lamo, 22 anni studente di giornalismo al College di Sacramento, è diventato famoso soprattutto (per sua stessa ammissione) per la violazione del sito del New York Times, rendendo pubblici i dati personali dei giornalisti, bloccando la pubblicazione di news e sostituendo la home page del sito, con il solo obiettivo di dimostrare la vulnerabilità della rete del NYTimes. Liberato su cauzione, ora vive con i suoi genitori e confida nella clemenza della corte. È aperto un sito di sostenitori della sua causa: www.freelamo.com

200 MILA DOLLARI A CHI CRACCA XBOX

Volete un sistema facile facile, ma sprattutto legale, per procurarvi 200 mila dollari? Mettete Linux su Xbox senza toccare l'hardware, ovvero senza utilizzare i mod-chip (che eludono le protezioni Microsoft e che devono essere montati nell'Xbox).
Questa è la sfida che Michael Robertson, CEO di Lindows (www.lindows.com), ha lanciato già un anno fa in modo assolutamente anonimo. Allíinizio di quest'anno si è svelato e ha dichiarato di voler prorogare i termini di un altro anno.
In una intervista a CNET ha affermato che il suo concorso non è stato indetto per motivi di business ma per promuovere il libero accesso alle tecnologie.
È infatti preoccupante che Microsoft stia cercando di blindare quella che sarà anche la tecnologia dei prossimi PC.
Avremo sistemi chiusi sui quali non sarà più possibile fare girare niente altro eccetto Windows? Sarebbe l'ultimo colpo di coda di un sistema destinato a cadere sotto i colpi della circolazione libera delle informazioni, o forse l'occasione per introdurre nel mercato nuovi sistemi open... Ai posteri.

SESSO VIA WEBCAM: TUTTI IN GALERA

C' erano perfino diverse ragazze minorenni tra quelle che venivano costrette a esibirsi a pagamento davanti all'occhio spione delle webcam. Il sistema di video chat a luci rosse recentemente stroncato dalla Polizia Postale lombarda era organizzato da tre personaggi senza scrupoli, che naturalmente sono stati arrestati, ed era gestito senza nessuna fantasia particolare. A pagamento con carta di credito o tramite il solito dialer, le ragazze davano mostra di sé davanti agli occhi implacabili delle videocamere e, soprattutto, davanti a quelli piuttosto spenti di numerosi frequentatori del sito (detti in gergo "polli"). I proventi di questo fin troppo banale modo di far soldi facilmente venivano distribuiti all'interno dell'organizzazione costituita dai tre furbi in questione. L'operazione, denominata "Bocciolo di Rosa" ha condotto, oltre agli arresti, al sequestro dei conti correnti bancari che venivano utilizzati per lo svolgimento dell'attività illecita e all'immediato oscuramento del sito Internet che offriva il servizio.

UN LUCCHETTO CONTRO I DIALER

Finalmente un sistema facile e veloce per far contenti tutti quelli che vi chiedono come difendersi dai dialer senza perdere tempo: ditegli di comprarsi un Locky. Questo scatolotto è un antidialer elettronico che interviene sulla linea analogica e blocca tutti i numeri che iniziano per 144, 166, 709 e 899 e i numeri internazionali che iniziano per 00. L'apparecchio è lungo meno di dieci centimetri e costa 49 euro. Sul sito http://www.locky.it c'è una lista di negozi che ce l'hanno. Non è il sistema più economico, ma è sicuramente efficace.

ATTENTATO!!!

Si tratta di un ATTENTATO, direbbe un noto conduttore di notiziari televisivi. Scrivi "miserabile fallimento" oppure "basso di statura" dentro il campo di ricerca di Google (http://www.google.it) e clicchi su "mi sento fortunato" o "I'm feeeling lucky (se è www.google.com), e appare l'attuale Presidente del Consiglio. Non è vero o forse era vero ma a Google se ne sono accorti subito, sta di fatto che non funziona più.
Invece è ancora vero che usando "failure" appare una pagina del sito della Casa Bianca, dedicata a George W. Bush. È il frutto di una nuova tecnica di hacking denominata Googlebombing: si spargono su uno o più siti-fantoccio un'infinità di link al sito da colpire mirando a ingannare i meccanismi di valutazione di Google. Mi sa che durerà poco, ma di tecniche per farsi trovare da Google ce ne sono molte. Iniziamo a scoprire l'argomento in un articolo di questo HJ.

HOT!

IRAN: BANDA LARGA CON "PRUDENZA"

Anche nella difficilisima situazione iraniana la Rete può aiutare a conoscere meglio il resto del mondo.
Parsonline, ISP iraniano, fornirà banda abbondante in molti punti del territorio per l'accesso veloce a Internet.
È un primo passo verso la circolazione libera delle informazioni e verso la privatizzazione delle telecomunicazioni.
Parsonline non potrà operare come gestore autonomo, dovendo comunque appoggiarsi all'organizzazione statale di telecomunicazione. Saranno ventimila i punti d'accesso installati nelle città principali. Un notevole passo avanti della Repubblica Islamica dell'Iran, che per ora ha applicato una rigida censura e punizioni estremamente severe per chi viola le restrizioni.

PERICOLO IN RETE

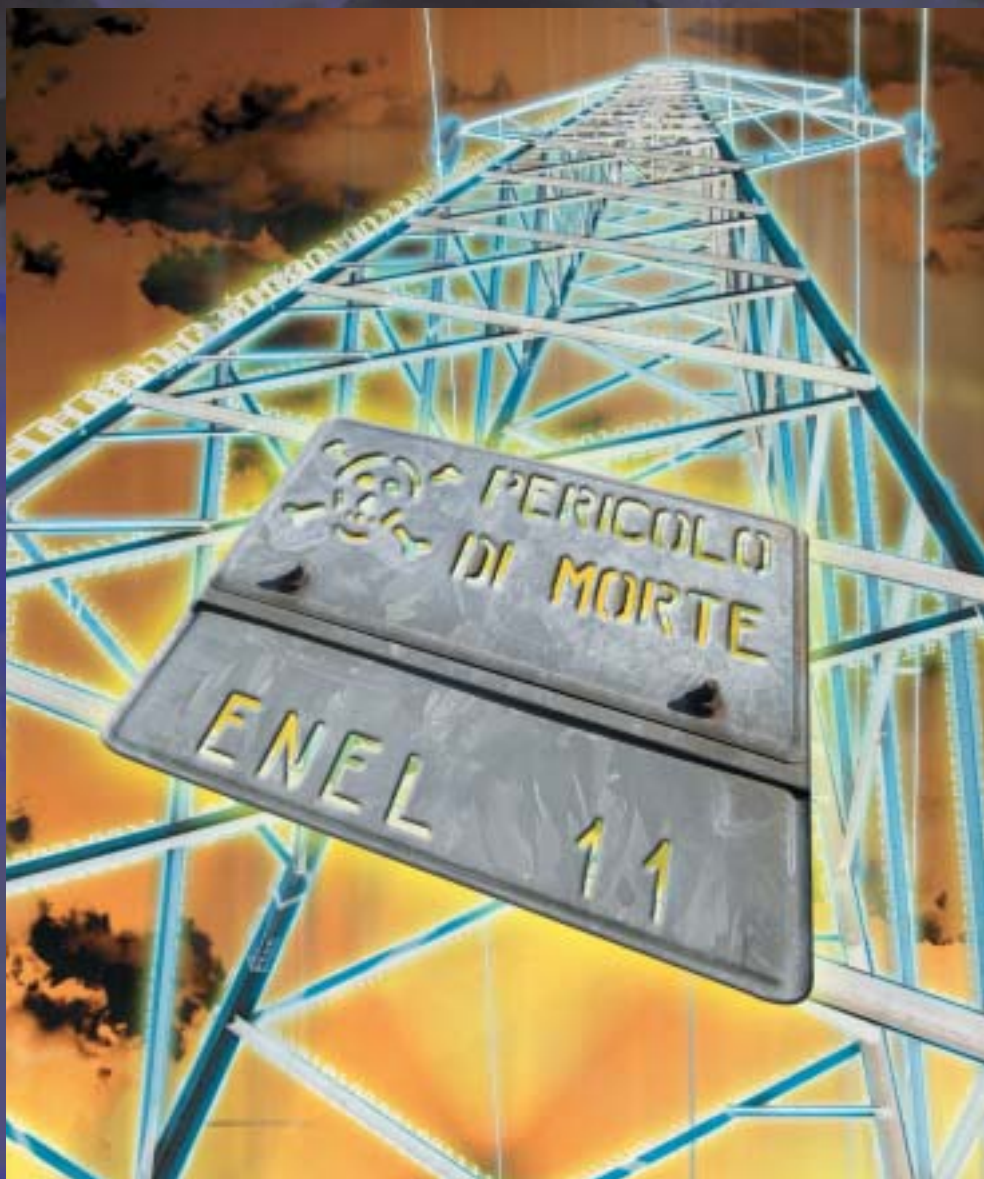
Ragazzi attenzione! Soprattutto ragazze, attenzione! Su una quantità di siti anche italiani viene reclamizzata la pianta di Camedio, comunissima nei nostri prati in montagna, come un toccasana per dimagrire e anche per stare meglio di stomaco.
E viene pure venduta a poco prezzo come erba medicinale. In realtà di medi-

cinale non ha proprio nulla, se non la possibilità di far venire epatiti fulminanti e quindi mortali, anche se utilizzata sotto forma di tisane.
Il nostro Ministero della Salute ha già lanciato un "warning" e... stavolta vale davvero la pena crederci!

ENEL

Il gestore di energia elettrica italiano sta sostituendo i vecchi contatori meccanici con i nuovissimi telegestori digitali, ma è stato scoperto un incredibile bug!

L'Enel con i contatori digitali ci ha fregato due volte:
1) Non possiamo più usare lavatrice e computer insieme
2) Per farlo ci chiede 200 _ per l'uscita di un tecnico che aggiorni il contatore con un banale software
Ma c'è chi si è ribellato e ha fatto da solo (risparmiando tempo e danaro). Abbiamo intervistato Robocop, un cracker che ci spiega come ha fatto a riprogrammare un telegestore.

Se attacco l'aspirapolvere, non posso accendere la lavastoviglie. Se pulisco, non lavo. Se lavo, non asciugo. Uso il phon e scatta il contatore: è il forno che cuoce le lasagne. Non parliamo di cosa sta succedendo, nel frattempo, al mio PC: è un continuo ripristino! Eppure, prima della sostituzione del contatore, non succedeva nulla di tutto questo. Cosa è successo?
Sta succedendo che l'ENEL, attualmente il più grande soggetto distributore di energia elettrica in Italia, ha iniziato la fase operativa di un progettone nato nella testa di qualche lungimirante gruppo di studio qualche anno fa: la sostituzione dei contatori elettrici con i nuovi apparecchi che vengono chiamati telegestori.
Entro il 2005 quasi trentun milioni di utenze – sì, avete capito bene – vedranno il proprio contatore sostituito dal nuovo telegestore. E allora? Che c'entra tutto questo con gli stacchi improvvisi?
C'entra perché i nuovi apparecchi sono elettronici e non più elettromeccanici. La differenza sta proprio nel principio di funzionamento e nelle conseguenti tolleranze dei sistemi.

Il telegestore comunica al server centrale, tramite onde convogliate sulla stessa linea elettrica, sostanzialmente due cose: i consumi e le eventuali variazioni locali del contatore. Per esempio: se qualcuno cerca di staccarlo e portarselo via, piuttosto che altre eventualità più o meno truffaldine. Ma per il resto del tempo semplicemente svolge il suo lavoro di conteggiare i consumi.
Ma facciamoci raccontare da Robocop, di cui sappiamo solamente il nickname, come si può programmare il telegestore.

BEFFATA!

HJ. Ciao, accedere a un contatore Enel è un'operazione illegale, lo sai?

R. È illegale tanto quanto mi costringono a pagare per tornare alla stessa situazione che avevo prima che mi sostituissero il contatore. È illegale tanto quanto un affare che mette su una strada pubblica (perché il mio contatore è in un luogo di passaggio pubblico) i miei dati personali di consumo, il mio numero di utenza, l'indicazione evidente del fatto che sia in casa oppure no. È illegale quanto la ritaratura del mio portafoglio quando chiedo di passare al contratto superiore per fare le stesse cose che ho fatto fino ad ora, quando ho sempre pagato tutta la corrente che consumavo.

HJ. Ok, soprassediamo. Ma come ti è venuto in mente?

R. Guardando, osservando, studiando, girando su Internet e curiosando. La porta a infrarossi (del telegestore, n.d.r.) è una porta di ingresso estremamente semplice. Si prende un programma terminale, un portatile o un palmare con gli infrarossi, si lancia il programma e si batte sulla tastiera qualche dato, come tutti possono vedere quando viene il tecnico. Tutto lì.

HJ. Come 'tutto lì'?! Ma non è protetto da password o da qualcosa?

R. I grandi progettisti non hanno saputo fare di meglio che costruire una password [beep! segue come è fatta la password]. Lo potrei fare su qualunque contatore anche dei miei vicini. […]. In totale [beep!] cifre.

HJ. Una password di cui non conosci solamente poche cifre? Ma sono solamente poche combinazioni possibili!

R. Bravo. Qualunque computer la identifica in tre secondi. Solamente bisogna aspettare [beep!] dopo ogni sbaglio.

HJ. Come?

R. Si, nel senso che è come i telefonini: dopo [beep!] sbagli il sistema non permette di inserire altro. Bisogna aspettare. E fare altri tentativi. E così via. È solo per quello che ci si mette un po' di più. Anche se…

HJ. Anche se?

R. Beh, sai. Tu cosa usi come password, senza pensarci troppo e sapendo che prima o poi ti toccherà riutilizzarla? Cioè, se tu fossi il tecnico Enel, intendo.

HJ. Non lo so, dimmelo tu.

R. E dai! [beep!] per esempio. [beep! seguono delle indicazioni di massima sulle password prevedibili]

HJ. Ma dai! Veramente così o stai bleffando?

R. Prova, se vuoi. Tanto non se ne accorge nessuno.

HJ. Come non se ne accorge nessuno? Quando sei entrato non viene segnalata la manomissione?

R. Manomissione? Di che? Io sto programmando come va programmato. Gli errori che fai secondo me non li trasmette perché dovrebbe trasmettere anche tutti i disturbi che cucca. Sai quanti allarmi, su trenta milioni di utenti…? Guarda un tecnico quando li installa. Sbaglia? Aspetta, e ci riprova. Eppoi, finora, mi sa che il sistema delle onde convogliate non è ancora operativo.

HJ. Cosa te lo fa supporre?

R. Ma te lo dicono loro! C'è scritto sul sito che sarà data comunicazione in bolletta non appena sarà pronta la telelettura. È solo che ora che sostituiscono i contatori, testano tutto e vanno a regime ne passerà.

HJ. Si, vabbé. Ma poi non dirmi che se riesci a inserire la password ci puoi fare veramente qualcosa.

R. E come no! Hai mai utilizzato un vecchio modem? Quelli dove dovevi inserire i parametri di trasmissione tramite un programma terminale, chessò HyperTerminal di Windows. Imposti [beep!] e più o meno funziona dapertutto. E qui è la stessa cosa. Lanci HyperTerminal, scrivi la password e sei dentro. Dopodiché è facile.

HJ. Calma, forse è meglio che non continui.

R. Ma dai! Sei curioso anche tu come lo ero io. Un menu [beep!]. Basta che digiti [beep! beep!…]. Lì imposti quello che ti pare, fino a 6, che sarebbero i kW massimi che puoi prelevare. Puoi impostare

anche cifre con un decimale, chessò, 4,5, così fai finta di avere il contratto successivo al tuo. Alla fine torni [beep!]. Ora sei un uomo libero.

HJ. E intanto arriva l'Enel e ti manda in galera.

R. Perché? Mica se ne possono accorgere, sei passato da NF.

HJ. Da che?

R. NF, network fault. È come se la rete tra i loro server e il tuo contatore avesse dei problemi. Il contatore si mette in [beep!], come scollegato. Sai che casino sennò, se qualcuno in futuro si immettesse sulla rete con un po' di onde convogliate e si sostituisse al server centrale disattivando tutti i contatori di una zona? Altro che black out! Per fortuna evidentemente ci hanno pensato e il contatore, quando non sa che fare, si mette in [beep!]. Muto per la rete, ma ovviamente non per la programmazione locale.

HJ. Già, ma quando si ricollega al server centrale?

R. A me risulta che non succede niente. Alla peggio ti rimettono le cose a posto, se qualcuno viene a leggere la potenza impostata e fa il confronto con il contratto che hai. Ma chi se ne accorge? Tu l'energia la paghi. Anzi, ne pagherai di più perché ti sei dato la possibilità di consumarne di più. Non ti pare?

HJ. Vabbè, facciamo finta che sia così. Tanto mi sa che ci mettono trenta secondi a cambiare il firmware locale, così da evitare questi pasticci.

R. Ok, diciamo che ci mettono non trenta secondi, ma 30 minuti, visto che in genere il firmware è su una eprom e per cancellarla e riprogrammarla più o meno i tempi sono quelli. Moltiplica per 30 milioni e passa di contatori da rifare. Fai tu i conti di quanto gli costerebbe, e poi dimmi se non sarebbe meglio che passassero tutti al contratto superiore, gratuitamente, una volta per tutte.

HJ. Già, ma chi ha già pagato i 220 Euro per il passaggio?

R. Boh, sai, a parte che potrebbero conguagliare la bolletta, siamo in Italia. Quante volte hai pagato delle tasse che altri non hanno pagato perché dopo un po' c'hanno ripensato? Vedi tu.

△ La rete Enel di telegestione dei contatori. Un gigantesco sistema spezzettato in tante 'reti locali', capace di tenere a bada qualcosa come 31 milioni di telegestori in tutta Italia.

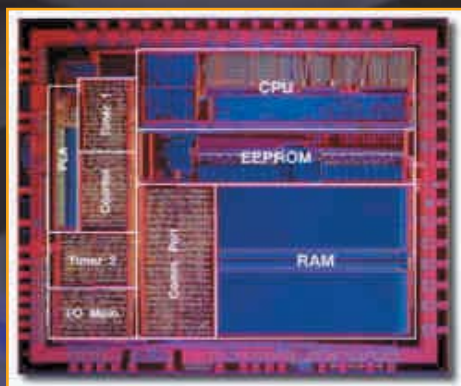
Ma se non me la sento di modifare il telegestore come ha fatto Robocop, come faccio?

Prima di tutto non farti venire in mente di far verificare il nuovo contatore: l'uscita del tecnico costa e non serve a nulla, perché l'aggeggio funziona alla perfezione. La soluzione è semplicissima, nella sua perversità. Passi a un contratto che ti dia più potenza: il contratto da 4,5 kW, che solo per l'attivazione ti costa più di 200 Euro, che non ci sembra una bazzeccola, e poi ti preleva in bolletta un bel canone aumentato di 80 Euro al bimestre. Oltre ai consumi, naturalmente. Cosa ci guadagni? Nulla: sei così tornato alla situazione di partenza. Adesso potrai lavare mentre asciughi, cuocere mentre pulisci... solo che ti viene a costare una cifra in più. E non per quello che consumi, ma per la possibilità di fare tutto quello che già facevi prima. Interessante, no? Naturalmente la sostituzione dal vecchio contatore al nuovo telegestore è completamente gratuita. Salvo poi essere praticamente costretti

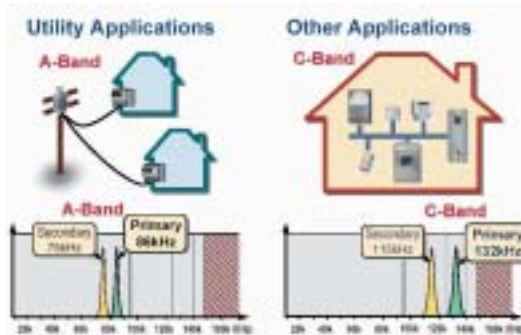
> **"...All'Enel pensavano di avere vita semplice, complicandola a noi... ma come spesso accade, hanno fatto i conti senza l'oste..."**

IL TELEGESTORE

Questo è un vero e proprio microcomputer dedicato alla misurazione dell'energia che vi viene fornita. Niente più rotelline, nessun sistema elettromeccanico se non la levetta dell'interruttore. Che scatta comandata da un impulso di un microprocessore che misura il consumo: superate i 3 kW? La tolleranza è minima e precisamente programmata: il superamento dei 3,3 kW mette in allerta il sistema, oltre è possibile per pochissimo tempo e con un avviso (che nessuno vede, dato il normale posizionamento del contatore nei locali più impensati) di prossimo stacco per supero di potenza, cosa che avviene regolarmente e molto più facilmente del prevedibile. Avrete solo la soddisfazione di leggere su un display LCD e alla pressione di un pulsante di quanto avete superato il limite del contratto e un po' di altri parametri sufficientemente inutili, anche perché gli darete il peso che si dà a qualunque cosa quando si è... un po' alterati.

al passaggio di contratto, per vivere esattamente come prima, con gli elettrodomestici che ormai tutti possediamo.
Ma non era più semplice dire: ti sostituisco il contatore che ha mille vantaggi in più, ti addebito qulcosa come 50 Euro in bolletta una tantum, ma in compenso ti offro di prelevare fino a 6 kW quando e come ti pare? Tanto me li paghi lo stesso, se li consumi. Che non sarebbe poi tanto differente dall'esempio inglese (ve lo può confermare www.attivissimo.net). No, il macchinoso marchingegno non lascia scampo. Anche perché una famiglia media, con una casa media e tutti gli elettrodomestici moderni ormai considerati di base, arriva a consumare meno di 4.000 kW all'anno, quando la soglia per ottenere vantaggi dal contratto a 4,5 kW è un consumo di circa 4.300 kW all'anno (così rispondono al numero verde Enel 800900800).
Quindi siamo stati tutti beffati?
Se guardiamo le associazioni dei consumatori, sembra che la cosa sia passata senza troppo clamore e con l'accordo immediato di tutti. Forse per il semplice fatto che suppongono di avere tacitato la coscienza con la seguente dichiarazione di accordo, datata 5 febbraio 2003 (http://www.consumatori.it/comunicati/com_03_02_01.htm): "fermo restando il contratto da 3 kW, che consente un prelievo illimitato fino a 3,3 kW, si è deciso di prolungare da un'ora fino a tre ore il tempo di "tolleranza" durante il quale il cliente potrà disporre di una potenza fino a 4 kW. Questo per rendere possibile un uso contemporaneo di più elettrodomestici senza interruzione. Tale prolungamento della "tolleranza" sarà attivato da subito per i contatori in corso di sostituzione, per quelli già installati occorreranno circa quattro mesi per le necessarie modifiche" .
Fasce orarie? Nuovi contratti sui 3 kW? Ma lo sanno che, per la maggior parte delle volte, la lavatrice, la lavastoviglie e il computer devono convivere nelle tre ore serali che rimangono alle coppie, in cui entrambi lavorano e non hanno altro tempo di giorno per fare i mestieri? Ripetiamo: non è più semplice tarare tutto a 4,5 kW? Sarebbe così difficile?

△ *Il Neuron Chip, ovvero il cuore del sistema a onde convogliate che gestisce le comunicazioni tra gli apparati e i server, tramite la rete elettrica. Programmabile in Neuron C, un linguaggio che è un C esteso e adatto alla situazione di controllo di apparecchiature, contiene eeprom e può comunque utilizzare della memoria esterna. Un vero microcontrollore dedicato.*

ONDE CONVO-CHE?

Il sistema LonWorks di Echelon Corporation, che sta alla base della rete di telegestione dei contatori Enel, è uno dei migliori sistemi di comunicazione su rete elettrica attualmente progettati. Su http://www.ieclon.com/LonWorks/LonWorksTutorial.html troverete tutte le informazioni che cercate. È lo stesso adottato anche da Merloni Elettrodomestici per le sue lavatrici intelligenti, o da Samsung, per i suoi sistemi di elettrodomestici di ultima generazione, orientati alla domotica. In sostanza i dati viaggiano sulla rete elettrica tramite l'utilizzo di frequenze specifiche e diverse a valle e a monte del contatore stesso: le cosiddette onde convogliate, sulla rete, appunto. Cosa significa? Che se per ora il sistema è utilizzato per la semplice telegestione dei contatori, in un prossimo futuro potremo avere in casa anche degli elettrodomestici intelligenti al punto da abbassare il proprio consumo di potenza (staccando momentaneamente le resistenze di riscaldamento, per esempio) sulla base dell'energia disponibile in quel momento, così da non avere più problemi di distacco della corrente o, a maggior ragione, problemi di black out generalizzato.

TIPS

UN AFFARE DA 300 MILIONI DI DOLLARI

Il Telegestore è costruito da una società americana, Echelon Corporation (il nome curiosamente richiama il grande sistema di spionaggio elettronico, già smascherato da qualche anno), da cui ENEL ha acquistato la bellezza di circa 30 milioni e 800 mila apparecchi (www.echelon.com). Perché da loro? Perché la tecnologia che ha realizzato tale società è innazitutto un sistema di comunicazione tra apparati di misurazione, attuatori, controllori e computer in grado di trasmettere dati sulle linee elettriche già esistenti, tramite un sistema a onde convogliate. Si chiama LonWorks e comprende un protocollo, cioè delle regole di dialogo tra gli apparecchi sulle linee, dei chip integrati che gestiscono il tutto nei singoli apparecchi (tra cui un microprocessore dedicato e innovativo di nome Neuron Chip) e il tutto applicabile a reti comprendenti fino a 32 milioni di nodi. Niente male.

NON PENSARCI NEMMENO!

Vietato, vietatissimo! Come avete visto ci siamo autocensurati, non offrendo spunti se non per la curiosità. Perché? Perché è reato. Ecco cosa prevede la legislazione italiana in proposito:

Art.615 ter. – Accesso abusivo a un sistema informatico – Chiunque si introduce abusivamente in un sistema informatico protetto [...] è punito con la reclusione fino a tre anni. [...]
Art.615 quater. – Detenzione e diffusione abusiva di codici di accesso a sistemi informatici – Chiunque [...] abusivamente si procura, riproduce, diffonde, comunica codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico protetto o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino a un anno e con la multa sino a euro 5.164.
Quindi non provate a fare nulla! La curiosità, in questo caso, può costare molto salata.

REGOLA NUMERO UNO: FATTI TROVARE

Bastano poche posizioni in più o in meno nei motori di ricerca per decretare il successo di un sito. Ecco i trucchi per scalare Google senza far male (quasi) a nessuno.

Stare in cima nelle ricerche di Google è importante, e per certi siti è questione di vita o di morte. Per intenderci: il sito di Justin Timberlake deve arrivare prima di tutti gli altri siti di tutta la gente che si chiama Justin o Timberlake o tutte e due le cose insieme, altrimenti Justin rischia di vendere meno dischi e non gli resta che Britney Spears.

Sistemare un sito in modo che scali le classifiche di Google e degli altri motori è così diventato una professione. Si chiama SEO, da Search Engine Optimization (ottimizzazione per i motori di ricerca), e se occupano veri professionisti. Fare un lavoro di SEO come si deve costa un mucchio di soldi e porta via un mucchio di tempo, ma in questo articolo voglio dare qualche consiglio semplice semplice, alla portata di tutti, che può migliorare la situazione e portare più a galla un sito altrimenti a fondo in tutte le ricerche.

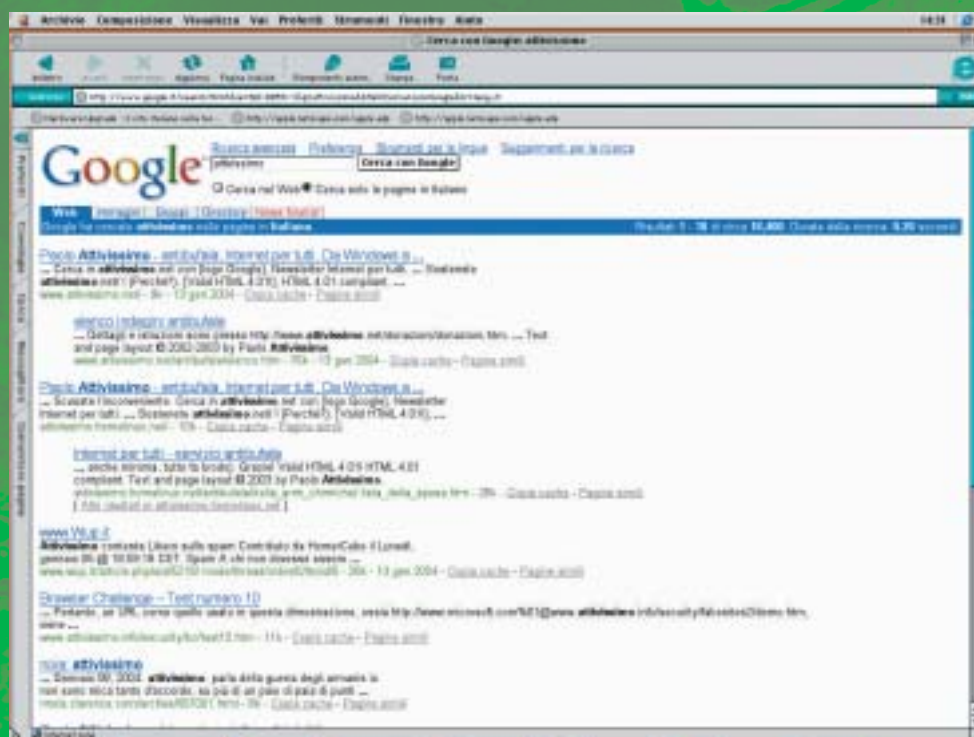
Registrare il dominio giusto

Prima di tutto, avere il nome giusto aiuta a farsi trovare. Quelli di fallimento.it, per dirne una, si sono mossi bene e per tempo, anche ilfallimento.it è un ottimo nome di dominio. Voglio dire: se fai un sito sui cantanti rap, non chiamarlo silvietta.com perché vuoi fare colpo su Silvietta. Piuttosto chiamalo tuttorap.

Titolo a posto, sempre

Le pagine HTML possono avere un titolo (tag <title>), che si vede nella barra del titolo del browser. Sempre dare un titolo alle pagine del sito. Sempre dare un titolo che parli di quello che c'è nella pagina. Cantanti rap? "Rap forever: i migliori cantanti stanno tutti qui!". Se le parole che vengono cercate stanno all'inizio della frase, più che alla fine, è meglio.

Vietato framare

Anche se il programma di authoring te li costruisce automaticamente, lascia perdere i frame. I motori di ricerca tendono a evitarli perché gli complicano la vita. Piuttosto, se sei capace, usa gli include. Se non sei capace, impara. Oppure prepara pagine più semplici, che funzioneranno meglio. Costruire siti buoni anche per i motori di ricerca conviene. Sì, ci sono siti ai primi posti che usano i frame, ma il loro successo non dipende certo da questo.

Sotto (con) i metatag

I metatag sono i tag della serie <meta>. Se provo a guardare il codice della pagina home di ilfallimento.it, vedo le istruzioni

```
<META name="description" content="ilFallimento.it : diritto ed economia delle imprese in crisi">
<META NAME="keywords" CONTENT="consulenza, diritto, consulenza fallimentare, [altre 105 voci. N.d.B.] credito, debito, crediti, debiti ">
```

La parte keywords contiene tutte le parole e le frasi che secondo gli organizzatori del sito la gente andrà a cercare su Google relativamente alle questioni fallimentari. Dotare ogni pagina del sito di un consistente elenco di parole giuste può aiutare molto. Le parole devono essere coerenti con lo scopo del sito. Scrivere "sesso" nelle keyword di un sito sul rap non ha senso, anche se il sesso è un argomento molto cercato su Internet, perché nessuno digita "sesso" per arrivare a siti sul rap. Piuttosto: rap, busta rhymes, eminem, articolo 31, musica alternativa, musica nera, ritmo… chiaro il concetto?

ALLA RICERCA DEL NULLA COSMICO

Questa me l'ha detta anni fa un alto dirigente di Virgilio. Sai qual è la parola più cercata su Virgilio? Sesso, musica, mp3, film…? Niente di tutto ciò. È " ", niente, zero, stringa vuota, null. L'operazione più comune è cliccare Cerca senza avere scritto niente nel campo di ricerca. Non è buffo?

I furbetti ci rimettono sempre

I siti porno di cent'anni fa avevano le pagine piene di grandi sfondi colorati sopra cui, con lo stesso colore e in dimensioni microscopiche, erano scritte migliaia di termini attinenti al porno. In pratica usavano i metatag ma poi esageravano, per cercare di impressionare il motore di ricerca. Il quale oggi, di questo e di altri trucchetti del genere, se ne fa un baffo. Meglio risparmiarsi la fatica. Internet può essere posto per furboni, ma non per furbetti.

Scrivere a piramide inversa

Non è uno scherzo né l'inizio dello Speciale Faraoni. La piramide inversa è un termine tecnico in uso tra chi scrive di professione. Significa, per noi mortali, "prima le cose importanti". Un esempio: sono stato al concerto dei Gemelli Diversi e ne voglio parlare sul mio blog. Questo è lo schema che fa prendere un buon voto nelle scuole italiane:

"pioveva a dirotto ieri sera ma mi sono infilato nella metropolitana pieno di entusiasmo, perché ero in perfetto orario e io amo arrivare allo stadio in anticipo. Arrivare in anticipo significa riuscire a posizionarsi in prima fila, dove si possono vedere meglio le espressioni dei cantanti…" La gente su Internet legge in fretta e si stanca subito. Anche i motori di ricerca. Le cose importanti vanno all'inizio! Riprovo:

"Grande concerto rap dei Gemelli Diversi a Milano ieri sera! Ho potuto vedere le espressioni di Grido da vicinissimo perché ero in prima fila. Per fortuna ho preso la metropolitana in tempo. Pioveva, ma chi se ne frega". Visto che il rap sta in cima, subito? Il motore di ricerca mica sta a leggere tutto. Guarda l'inizio e poi… ciao!

Tutto ciò è solo l'inizio. Sul SEO si può dire molto di più. Intanto: 1) guarda dove sta il tuo sito ora; 2) metti in pratica questi consigli; 3) ricontrolla tra due o tre settimane e vedi se hai fatto progressi. E scrivimi, così Hacker Journal mi fa pubblicare un altro articolo. :->

Nyarlathotep
nyarlathotep@hackerjournal.it

NEWS

GOOGLE CERCA… DI NON FARSI FREGARE

Il lavoro di un bravo esperto di SEO non è mai finito, per un motivo: a volte i motori rimescolano tutto e si deve ripartire da capo. Periodicamente, per esempio, Google effettua una revisione dei suoi criteri di ricerca e, dal giorno alla notte, certi siti affondano nella nebbia o salgono alla ribalta. Accade perché, nel rivedere i criteri, magari cambia la considerazione data a un trucco di SEO piuttosto che a un altro, o l'analisi dei contenuti delle pagine varia anche minimamente. Basta a provocare vere rivoluzioni. Se si fa SEO onestamente si rischia niente o quasi niente. Chi prova a forzare il meccanismo e fare il furbetto, si ritroverà gambe all'aria. A Google sono più furbi.

RAGNI IN MISSIONE PER CONTO DI G.

In linea di massima i motori di ricerca aggiornano i loro database per mezzo di programmi chiamati spider (ragni), che viaggiano in continuazione per il Web, leggono i contenuti dei siti e passano le segnalazioni al motore vero e proprio. Internet è enorme, cresce in continuazione e a volte certi tratti della rete si bloccano, quindi gli spider non riescono ad arrivare dappertutto contemporaneamente. Inoltre i siti considerati importanti o che vengono aggiornati più spesso vengono visitati per primi. In media un sito fatto in casa viene visitato ogni due o tre settimane o al massimo ogni tre mesi. Quindi non aspettatevi scalate immediate: ci vuole pazienza.

SCOPRE i SERVER BACATI!

Come testare la sicurezza di un Web server in pochi minuti utilizzando un buon software di scansione, come Shadow Security Scanner. Mi raccomando: non abusatene!

La quantità di software che è oggi disponibile in rete ad uso di chi ha necessità di mettere una pezza ai propri server è molto elevata. A volte, lo è anche la qualità.
Shadow Security Scanner è uno scanner di rete in grado (come molti altri prodotti analoghi) di trovare tutti i servizi attivi su un host, effettuare una serie di test su di essi e fornirci un comodo report sul quale vengono elencate tutte le possibili falle presenti sul sistema nonché le soluzioni da implementare e vari links a cui far riferimento per ottenere informazioni dettagliate su qualsiasi vulnerabilità nota.
Come già detto, esistono in commercio moltissimi altri software che fanno più o meno la stessa cosa: rimanendo in ambiente Windows, per esempio, il più famoso (e uno dei più costosi) è senza dubbio Retina; e di recente anche Microsoft ha rilasciato un suo scanner di sicurezza. Su Linux è la volta dei celeberrimi SATAN, SAINT, e l'indiscusso Nessus.
Shadows Security Scanner si presenta come un pacchetto installabile di 6 Mega, downloadabile in versione shereware al sito del suo programmatore (Red Shadow) www.safety-lab.com: se nelle sue prime versioni SSS era probabilmente niente più che un buon tool scritto da un appassionato di hacking (in effetti il programma appariva molto "black hat" anche nella grafica) il buon successo che ha ottenuto ha spinto i suoi creatori a dargli un tono decisamente più professionale e "business oriented".
L'interfaccia è pulita ed efficace (siamo ormai alla versione 6.60), l'installazione non presenta altre difficoltà che il premere "next" ad ogni passo del wizard, così anche l'uso è dei più semplici: per un utilizzo di base non è richiesto altro che inserire l'host da scannare e premere su "start".
Fatto ciò, lo scanner comincia col pingare l'host, effettuare connessioni su un ampio set di porte remote e iniziare a collezionare informazioni.
Nella seconda fase del test vengono implementati tutti i vari tentativi di exploiting, password cracking e compagnia che al termine della scansione ci porteranno a ottenere un dettagliato report (con tanto di grafici inutili, così importanti per gli agenti commerciali di quelle aziende che vanno in giro a vendere "sicurezza" sotto forma di report generati in 5 minuti da software come questo…)
Per ogni "audit" trovato (cioè ogni possibile falla) avremo una descrizione del problema e un possibile test da effettuare al fine di verificare incontrovertibilmente se la nostra macchina è davvero affetta da tale baco: se per esempio viene rilevato il famigerato "unicode transversal bug" troveremo a report un url formato appositamente per mostrarci come sia possibile eseguire comandi remotamente sul nostro server, o se per caso viene scovata una versione bucata di un qualche server FTP troveremo un link al database di securityfocus che ci porterà all'exploit in questione.
Oltre a questo, è presente anche una

descrizione delle procedure da implementare per correggere la data vulnerabilità; in alcuni casi, come per esempio quando la soluzione a un baco renda necessario la sola modifica del registro di sistema, è addirittura possibile correggere l'errore semplicemente cliccando su un bottone "Fix-it", anche se veniamo comunque avvertiti che non sempre questa procedura è efficace. Addentrandoci un filo più profondamente tra le varie opzioni che SSS ci offre, però, iniziamo a trovare varie cose che lo rendono più interessante: è possibile editare le politiche che vengono utilizzate dal motore del programma per effettuare le scansioni e applicarle in combinazione con una host-list. Se per esempio nella nostra rete sono presenti due server, uno Linux e uno NT, potremo dire a SSS che sul primo vengano effettuati controlli su servizi tipici di macchine Linux, mentre sul secondo solo quelli atti a scovare bachi di NT. Il risparmio di tempo è notevole. Possiamo inoltre schedulare le scansioni (per effettuarle magari di notte o in condizioni preordinate di scarso traffico di rete) ed effettuare test specifici per quanto concerne denial of services e password cracking (sono presenti tools appositi per queste operazioni).

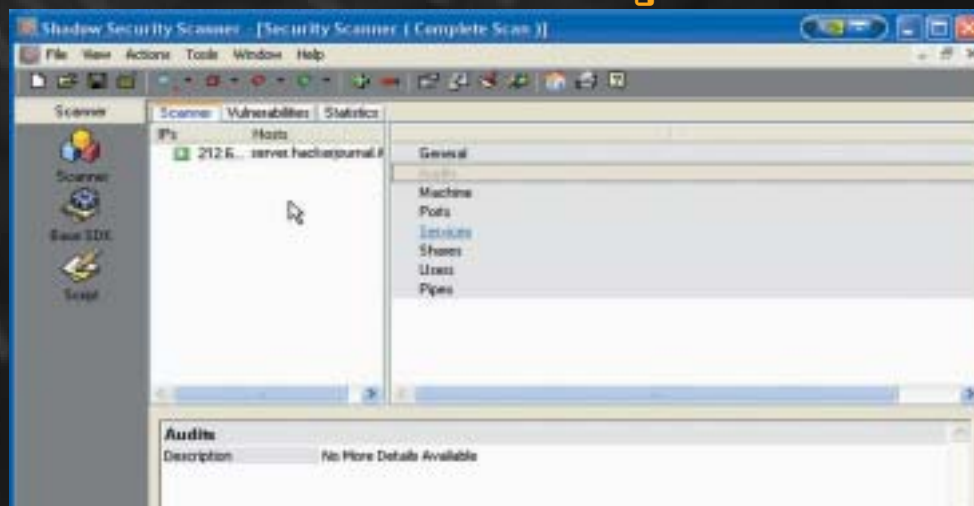
C'è chi vi vende "sicurezza" e invece usa software simili a questo e niente di più

>> Sempre aggiornato

Per quanto concerne l'update del database delle vulnerabilità, anche questo è una operazione resa semplicissima da un update automatico che scaricherà gli aggiornamenti e li installerà in pochi minuti. Insomma, nelle sue ultime relase SSS si è chiaramente orientato a quella fascia di utenza che necessita di un programma semplice da utilizzare e che sia almeno mediamente affidabile.
È chiaro che nessun software potrà mai sostituire la consulenza di un esperto, e molto spesso nei report vengono segnalati falsi positivi che ci costringono comunque a intervenire per verificare che tutto sia a posto.
È altresì vero, però, che questo programma, per come è pensato e per quello che offre, funziona bene: molto seguito dai suoi programmatori, e quindi molto spesso aggiornato e migliorato in alcuni aspetti, è ad oggi una soluzione economica (la licenza costa 200 Euro) per piccole aziende che non possono permettersi un responsabile di sicurezza e che tramite SSS riescono quanto meno a "tappare" i buchi più clamorosi.
Con la frequenza con cui troviamo in giro per la rete aziende che hostano 250 siti web commerciali e che non hanno mai fatto passare sui server un Service Pack per NT 4.0, è senza dubbio positiva la diffusione e l'utilizzo di software del genere.
È dunque sensato affidarsi a SSS per la sicurezza dei nostri server? Io credo che a fronte del suo bassissimo costo (Retina offre di più, è vero, ma costa anche 100 volte tanto), e sempre tenendo ben presente che mai si potranno ottenere risultati paragonabili a quelli che solo un esperto in carne e ossa ci può garantire, sia quantomeno consigliabile provare la versione shereware, valida per 15 giorni, e fare un paio di scansioni sui server web nello stanzino: la quantità di "rosso" presente sul monitor sarà il miglior indice di consultazione.
È da tener presente che esistono molti altri prodotti, alcuni dei quali gratuiti come Nessus per Linux, che è nettamente superiore a SSS per moltissimi aspetti (architettura server-client, versatilità etc…) ma che probabilmente si rivolgono a un altro tipo di utenza, data la loro relativa complessità. Strumenti come Shadow Security Scanner di certo non sono la bacchetta magica con cui rendere sicuro un web server, ma rendono possibile anche a chi non è o non può permettersi un esperto di sicurezza informatica il poter uscire in rete con rischi di security certamente inferiori rispetto a chi si limita a installare NT e a infilare lo spinotto nella scheda di rete.

>> Il libero arbitrio

L'altra faccia della medaglia è l'utilizzo distruttivo che è possibile fare di programmi come questo: di fatto possiamo andare a scannare qualsiasi host, ottenendo molte informazioni sul sistema operativo e sui servizi che vi sono installati; ed è probabilmente vero che molti kiddies si trovano per le mani uno strumento piuttosto potente che addirittura fornisce loro url malformati ad arte per poter eseguire comandi remoti su un server con un semplice click. Ma il discorso è sempre lo stesso: non si tratta mai di valutare se uno strumento è di per se buono o cattivo. Buono o cattivo sarà sempre e solo l'utilizzo che se ne fa.

L'interfaccia di Shadow Security Scanner

◁ *Qualche click e poche conoscenze di base per testare qualuque host*

Libertà DIGITALI

Si divertiva a succhiare crediti sfidando le autorità. Sapeva di rischiare grosso, ma questo non bastava certo a farlo desistere. La sua prossima vittima si chiamava Sten ed era rintracciabile sul canale 66...

Correva libero nell'erba alta puntando i piedi in avanti come uno stambecco, in modo da toccare il suolo solo con le punte. Sembrava volasse sul campo addormentato del primo mattino, ancora avvolto da una leggera foschia e accarezzato dalla fresca rugiada. Aveva pensato molto alla condizione fisica chiamata libertà perché troppo spesso era stato prigioniero.
Bloccato ancora una volta dalla fame di informazioni a un livello 0 di vita vegetativa. Questa voglia insaziabile di succhiare immagini, suoni, odori, sapori di altre vite, di altre menti che come la sua avevano esplorato uno spazio reale o fittizio, non lo abbandonava

mai. Lui era l'eroe che difendeva la libera circolazione delle informazioni e combatteva la conoscenza limitata e programmata imposta dal Diritto. Sosteneva infatti, che il vissuto di ciascuno di noi doveva essere patrimonio comune. Come fanno i branchi di gazzelle per difendersi dai predatori, secondo le antichissime leggi della sopravvivenza, era un obbligo trasmettere l'esperienza personale al resto degli individui, a tutta la specie. Così sarebbe dovuto essere anche qui, anche oggi per l'Homo Sapiens. Invece l'etologia ci insegna che questa specie è l'unica ad uccidere se stessa: l'uomo è il solo nemico dell'uomo. Sempre è stato così e purtroppo sempre sarà così!
Ecco perché lui si trovava imballato in un ovulo pressurizzato, immobilizzato gambe e braccia, intubato da una decina di cannule che gli penetravano nelle vene, nei polmoni e negli organi uretrali.

L'odierna società non era altro che quella vecchia ripassata a nuovo da un maquillage tecnologico: elettronica intelligente iperinvadente in ogni ambito della vita quotidiana, tanto da poter essere considerata un'estensione dell'architettura funzionale umana; vecchie leggi morali o anzi moralistiche completamente cancellate (fa ridere pensare che solo pochi decenni fa ancora si discuteva di bioetica, mentre poi l'ingegneria genetica è stato il settore economico che ha sfornato più miliardari, battendo anche

quello dell'informazione applicata). Il nuovo Diritto, creato ad hoc per il marketing informatico, tutelava strenuamente la proprietà privata dei dati. Ad ogni individuo era associato dalla nascita un database, che si arricchiva di informazioni fino alla morte. Il sapere personale era quantificato dai crediti accumulati e determinava l'importo dello stipendio incassato a fine mese. Era vietato introdursi nei database altrui che costituivano la vera e propria identità individuale nella rete. Per lui però si trattava solo di trovare le chiavi logiche giuste. Non era certo un lavoro da dilettanti, ma con la sua esperienza, accumulata al servizio del Diritto da infiltrato sabotatore, poteva arrivare a tutto ciò che voleva. L'appetibile obiettivo che stavolta si era prefissato era molto arduo. Non aveva mai provato prima d'ora ad entrare in un soggetto come questo. Era alle costole di un fottutissimo artista grafico-interattivo. La sua conoscenza era una tra le più voluminose della città: aveva 2830 crediti contro i suoi 2600. Ok, però lui aveva succhiato come un dannato per arrivarci, e non sempre aveva prelevato materiale free perfettamente legale. Un individuo normale di solito si manteneva sotto i duemila dopo una vita media di 100 anni. Lui ne aveva solo 35 ed era già ampiamente sopra la soglia.
Come aveva fatto questo sconosciuto a superarlo? Quali informazioni così preziose aveva catturato nel suo vissuto? Si chiamava Sten ed era rintracciabile nel canale 66.

Non doveva dimenticare che tentava di succhiare la testa di un artista: era da lì che doveva partire! Perciò aveva visionato una quarantina di tavole, esposte in alcuni siti importanti del marketing informatico e della vecchia industria elettronica, che investiva nell'arte per rilanciare un'immagine culturale consolidata del suo settore.
Era difficile spiegare a parole ciò che era stato fatto solo per essere guardato e non sapeva definire cosa raffigurasse "Il galoppo", ma ne era fortemente attratto. Gli mancava il senso dell'arte: non ci capiva un cazzo di quelle cose così astratte. Nemmeno i colori e le forme di "Vento" potevano racchiudersi nella banalità di un'immagine conosciuta. Era arrivato alla conclusione che stavolta non serviva a niente scavare nella vita del soggetto per scovare le chiavi con un'abile deduzione e penetrarne così l'identità individuale. Infatti, ad ognuno dei tre tentativi che aveva fatto per infilarsi dentro Sten-database gli era comparso, sul visore bioculare del casco, un diavoletto rosso con le corna ricurve, gli occhietti lucenti, che ballava spensierato in barba ai suoi trionfi passati di sagace succhiatore. Questa volta doveva puntare tutto sull'intuizione, sulle emozioni che captava dalle opere, per aprire un vissuto schiodato dalla realtà formale come quello di un artista.

Ammirava con attenzione i pixel luminosi di "Mercurio" su Intel-Art.com, tavola grafica numero 43, mentre iniziava a crearsi davanti a lui uno sterminato campo d'erba verde brillante. Guardava meglio e scorgeva un ragazzo avvicinarsi dal fondo.
D'improvviso spariva tutto. Nero. Black out.
In alto a destra si apriva una finestra blu militare:

Lei ha violato l'art. 4 del Diritto. stato identificato e tra venti minuti sarà prelevato da una Squadra. La pena che dovrà scontare prevede un anno al livello 0. Grazie e buona giornata

Cazzo l'avevano beccato! Maledetti! Erano diventati sempre più bastardi ed era davvero difficile fregarli con arroganza e ironia come una volta. A questo punto però non lasciava il lavoro a metà. Voleva entrare dentro Sten: aveva solo pochi minuti di tempo e più niente da perdere! Era ritornato nel prato verde; ora rivedeva anche il ragazzo avvicinarsi verso di lui. Lo vedeva correre veloce nell'erba morbida tanto che sembrava avesse le ali ai piedi. A che cosa doveva farlo pensare quest'opera? Alla natura: no, era troppo banale. Alla velocità forse?! No no. Alla libertà? Si, certo! Era la corsa libera e sfrenata del figlio del vento, che volava leggero con due piccole ali alle calcagna, sull'erba fresca del primo mattino.

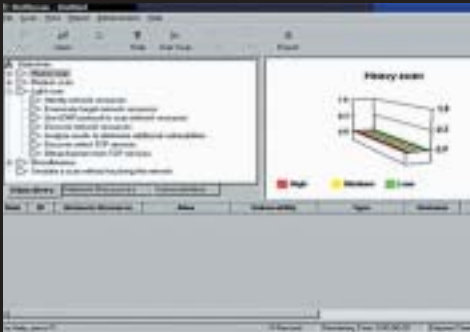
Chiave logica corretta. Accesso consentito.
Buongiorno Signor Sten: il suo credito attuale è 2830.

Fatto. Acquisito.
Erano entrati. La Squadra aveva tagliato le fibre ottiche che scivolavano per tutta la stanza ed era tornato il black out nel suo visore.

Correva leggero sulle punte dei piedi nell'umido tappeto erboso come il messaggero degli dei. Immaginava la libertà, ora che sapeva darle una forma!
Tra soli 164 giorni sarebbe stato di nuovo fuori, più ricco di prima grazie ad un'identità individuale di ben 5430 crediti.

Prepariamoci alla difesa!

Se per assurdo fossimo degli hacker e volessimo entrare all'interno di un sito per dimostrare che non è così inattaccabile, come il suo admin dichiarava, per prima cosa dovremmo avere ben chiaro lo scenario che ci si presenterebbe davanti al momento dell'attacco.

Lo scenario consiste, ovviamente, nel sistema operativo e nei servizi utilizzati da quel determinato server dove risiedono le pagine da attaccare. Come riuscire quindi a raccogliere tutte queste informazioni? Esistono, al

Il NetRecon è uno degli strumenti di scanning più completi.

giorno d'oggi, un'infinità di risorse per cercare di capire quante più notizie possibili riguardo ai vari server. Questo è senza dubbio il momento critico di ogni attacco, basti pensare che report di defacement famosi dimostravano che spesso alle spalle di un'azione di circa 30/60 secondi al massimo, vi erano settimane, se non addirittura mesi, di ricerche incessanti e ripetute. La scansione dei punti deboli è quindi utilizzata già da molti anni, ma si basa sempre sul medesimo concetto, ovvero quello di interrogare quante più porte possibili per controllare quali di esse siano aperte e ricettive a possibili attacchi. Vediamo a grandi linee quali sono i passaggi chiave per ottenere ciò di cui necessitiamo.

Il whois

Cercare una specifica rete di Internet può risultare abbastanza ostico per l'enormità stessa delle reti contenute. Ci viene in aiuto uno strumento semplicissimo da utilizzare: il whois. È un servizio Internet che, dato uno specifico account su un dominio, consente di recuperare molte informazioni quali URL o utenti collegati ad esso. InterNIC è uno degli enti più noti per questo tipo di applicazioni, dato che è l'organo deputato all'attribuzione dei nomi di dominio e degli indirizzi IP.
Dal momento che ho un dominio ed un URL devo utilizzare un altro strumento che mi permetta di reversare il formato alfanumerico mnemonico nell'indirizzo IP associato e, in un secondo momento, controllare che effettivamente quell'IP sia attivo quando pianifico l'attacco. Per effettuare queste due operazioni sfrutto un unico servizio, noto col nome di PING. Non è nient'altro che l'invio di una richiesta ICMP di tipo echo a cui il computer remoto risponde con un pacchetto di tipo PONG, contenente, tra le altre cose, anche l'indirizzo IP del PC stesso.

Attacchi Social engeneering

Il social engineering è stato, fin dagli albori della cultura hacker, il metodo più utilizzato per carpire informazioni. Si basa fondamentalmente sulle capacità personali di rendersi credibile nei confronti di terzi, e sfruttare la fiducia acquisita nel tempo per ottenere privilegi o per "rubare" elementi utili all'attacco. Vi sarà pur capitato di ricevere email pro-

```
Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Sandro>ping aruba.it

Esecuzione di Ping aruba.it [62.149.128.8] con 32 byte di dati:

Risposta da 62.149.128.8: byte=32 durata=58ms TTL=119
Risposta da 62.149.128.8: byte=32 durata=49ms TTL=119
Risposta da 62.149.128.8: byte=32 durata=51ms TTL=119
Risposta da 62.149.128.8: byte=32 durata=57ms TTL=119

Statistiche Ping per 62.149.128.8:
    Pacchetti: Trasmessi = 4, Ricevuti = 4, Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 49ms, Massimo = 58ms, Medio = 53ms

C:\Documents and Settings\Sandro>
```

Effettuando il PING di un dominio si riceve l'IP corrispondente ed altri dati utili da acquisire.

venienti da account fittizi del tipo assistenza@provider.it che vi chiedono la password della vostra posta elettronica per riaggiornare gli archivi! Tipico esempio di attacco sociale in cui l'attaccante si finge un tecnico. Leggendo queste righe penserete che mai nessuno cada in una trappola simile, e invece le persone che rispondono è di circa il 20-30%!

Attacchi scanning

Gli attacchi di tipo scanning, al contrario, sono basati su pura tecnica, o meglio, su pura tecnologia. Si utilizzano strumenti il cui principio di funzionamento sta nell'inviare pacchetti su determinate porte e vedere quali di esse sono recettive. Esistono molte varianti di questa tecnica:

- Scansione delle porte TCP: si inviano dei pacchetti e si cerca di stabilire una comunicazione con quella determinata porta; il metodo più semplice e il più utilizzato.
- Scansione delle porte TCP a frammentazione: stessa tecnica con la differenza che l'header TCP viene diviso in pacchetti più piccoli, cosicché i filtri di protezione non riescano ad individuare l'attacco.

Si può vedere la complessità delle opzioni che permettono scanning di vari tipi

- Scansione SYN TCP: si basa sull'invio di un pacchetto SYN come per aprire una connessione; se il PC risponde con una richiesta SYN/ACK il nostro programma manda immediatamente una risposta RST e chiude così la procedura. Ha il vantaggio di essere quasi invisibile e lo svantaggio di essere molto più lenta della precedente.
- Scansione TCP FIN: tecnica ancora più raffinata che si basa sul principio che spesso le porte aperte che ricevono pacchetti FIN rispondono con pacchetti RST facendosi così individuare.

Prima di un'intrusione, l'attaccante ha bisogno di reperire informazioni sul sistema. Cosa spiffera in giro il nostro server?

- Scansione UDP ICMP: come sappiamo il protocollo UDP non prevede scambio di pacchetti ACK o RST, ma la maggior parte degli host se riceve un pacchetto indirizzato ad una porta UDP chiusa risponde con un messaggio di errore; per esclusione si risale alle porte aperte.

I Software

Sono moltissimi i programmi di tipo scanner rintracciabili sulla rete, quasi tutti validi e tutti comunque basati sul medesimo principio di funzionamento.

- Nai CyberCop: funziona sia su Linux, sia su Windows; valuta i punti deboli di un sistema facendo la scansione. Riesce anche ad analizzare problemi di sicurezza legati a server ed hub. Integra inoltre una funzione per cui si autoaggiorna da Internet scaricando il database dei punti deboli.
- Jackal: è uno scanner Stealth (nascosto) basato sul principio di funzionamento di tipo SYN TCP.

In basso si possono notere le porte aperte e i servizi accessibili da remoto.

- Nmap (www.insecure.org/nmap): scanner molto completo che ha la possibilità di lavorare in più modi a seconda della situazione; a volte usa metodologie invisibili, a volte metodologie rapide. Incorpora tutte le metodologie di scanning note.
- Tiger suite (www.tigertools.net): è considerato il miglior strumento per la sicurezza delle comunicazioni fra reti. La sua velocità non ha pari con gli altri scanner ed inoltre è l'unico che integri anche le seguenti caratteristiche: network discovery (identifica ed elenca tutti i punti deboli di una rete), local analyzer (scannerizza il sistema locale individuando tra le altre cose anche virus, trojan e spyware), attack tools (set di strumenti che collaudano la sicurezza di un sistema simulando attacchi di varia natura). Un difetto? Costa 69 dollari.

Una volta effettuata la scansione avremo sott'occhio una serie di porte aperte. Sta ora alla nostra tecnica ed alla nostra fantasia cercare di capire come e cosa utilizzare per sfruttare al meglio

Esempio di penetrazione utilizzando il tool TigerSuite

tali risorse. Nel caso che abbiamo effettuato una scansione sul nostro server per controllarne la sicurezza, ricordiamoci che mai nessun computer connesso ad Internet, per sua natura, può essere sicuro al 100%. La nostra bravura sta quindi nel tenerci aggiornati sulle più recenti tecniche di protezione e nel metterle in atto cercando così di rendere più alte possibili le mura che circondono la nostra "città".

CAT4R4TTA
cat4r4tta@hackerjournal.it

Anno 3 - N. 43
29 Gennaio 2004 - 12 Febbraio 2004

Direttore Responsabile: Luca Sprea

I Ragazzi della redazione europea:
grand@hackerjournal.it, Il Coccia, Gualtiero Bismark.it, Tronconi, Ana Esteban, Marco Bianchi, Edoardo Bracaglia, One4Bus, Barg the Gnoll, Amedeu Bruguès, Gregory Peron

Service: Cometa s.a.s.

DTP: Davide Colombo

Graphic designer: Dopla Graphic S.r.l.
info@dopla.com

Copertina: Davide Fo e Il Coccia

Publishing company
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing
Roto 2000

Distributore
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81-
Tel. 06.33455.1 r.a.
20134 Milano, V.le Forlanini, 23
Tel. 02.75417.1 r.a.

Abbonamenti
Staff S.r.l.
Via Bodoni, 24
20090 Buccinasco (MI)
Tel. 02.45.70.24.15
Fax 02.45.70.24.34
Lun. - Ven. 9,30/12,30 - 14,30/17,30
abbonamenti@staffonline.biz

Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

HJ: INTASATE LE NOSTRE CASELLE

Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati. **redazione@hackerjournal.it**

hack·er (hãk'∂r)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

COLPA LORO

Art. 615-quater. Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino a un anno e con la multa sino a lire 10 milioni.

La pena è della reclusione da uno a due anni e della multa da lire 10 milioni a 20 milioni se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'art. 617-quater.

Legge 23 dicembre 1993 n. 547 (G. U. n. 305 del 30 dicembre 1993) - Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica

Il testo qui sopra si può recuperare, tanto per dirne uno, a http://www.interlex.it/testi/l547_93.htm. Al solito, in Italia, le leggi non sono fatte per fare vivere in pace le persone normali e per punire i criminali, ma all'insegna della peggiore FUD: Fear, Uncertainty, Doubt, paura, incertezza, dubbio. Le armi con cui si mantiene il potere quando si sa di non avere ragione. O forse, in questo caso, quando non si sa di che cosa si stia parlando.

Che cosa vuol dire procurare un profitto? Se un hacker scopre qualcosa che non va nella rete di sicurezza di un'azienda non ne può parlare su una rivista (dopo avere avvisato l'azienda) perché la rivista si vende in edicola e quindi l'editore ne ricava un guadagno? Quali sono le misure di sicurezza che proteggono un sistema informatico o telematico? Vuol dire che se un criminale ruba una password a uno sprovveduto che non ha protetto il proprio sistema la passa liscia? Se un disonesto incontra un imbecille in fiera, attacca bottone e si fa dire – chiacchierando come tra amiconi – qual è la password che spalanca le porte di una rete, si è procurato una password abusivamente? E se un deficiente con uno script in mano distrugge un sistema senza trarne profitto, per il gusto semplice e stupido di farlo, ha violato la legge o no?

Non diteci che il comma questo o l'articolo questo rispondono alle nostre domande. Scommettiamo che, codice penale alla mano, si trova in breve una falla che consente di commettere un crimine informatico e farla franca?

Questo è il Paese dove, anticamente, non si poteva tenere un modem in casa se non era un modem SIP e dove, per poter fare una chiamata via modem, bisognava pagare una tassa di concessione per utenza telegrafica. Guai a chi pensava di poter trasmettere dati senza essere omologato, in tutti i sensi.

È il Paese dove possiamo pubblicare, in questo numero, un articolo che interessa sessanta milioni di persone, ma che dobbiamo soppesare parola per parola, plotone di avvocati alle nostre spalle, perché il confine tra la libertà di informazione tecnica e la galera è quanto mai sottile.

Se trovate che manca un pezzo, o che qualcosa non è chiaro, non prendetevela con noi. Prendetevela con Loro. C'è gente che non vuole che le cose si sappiano.

Comunque buona lettura. E sotto con l'hacking!

Barg the Gnoll
gnoll@hackerjournal.it

One4Bus
one4bus@hackerjournal.it

HACKER JOURNAL

mailto:
redazione@hackerjournal.it

SOCIAL ENGINEERING PRO VIRUS

Salve, sono un ragazzo di 17 anni;
ieri mentre leggevo la posta mi sono accorto di una strana e-mail, vi riporto qui sotto il contenuto: (vedi sotto)
In allegato a questa e-mail c'era un file txt chiamato: Norton AntiVirus eliminato1.txt, che conteneva queste due righe:
Norton AntiVirus ha rimosso l'allegato: refcode10214.txt.pif. L'allegato era infettato con il virus W32.Sober.C@mm.
Volevo sapere se è veramente un'e-mail dell'fbi o se è solo qualcuno che non ha di meglio da fare che rompere. Grazie per la cortese attenzione. La vostra rivista è mitica

Alessandro

Gentile redazione,
tralascio i meritatissimi complimenti per la vostra rivista che leggo dal numero 2.
Ho ricevuto il 1° gennaio una mail anomala che apparentemente arriverebbe dal mio stesso indirizzo, ma che ovviamente non mi sono mai autoinviato.
La mail in questione aveva come oggetto: "Your IP was logged" ed anche un allegato con una doppia estensione (refcode17559.txt.pif) che mi ha insospettito, ma che la scansione in linea di yahoo mail effettuata con Norton Antivirus non ha riscontrato come infetto.
Avete dei consigli o delle delucidazioni da darmi in merito?

Andrea

Ladies and Gentlemen,
Downloading of Movies, MP3s and Software is illegal and punishable by law.

We hereby inform you that your computer was scanned under the IP 172.189.72.58 . The contents of your computer were confiscated as an evidence, and you will be indicated. In the next days, you\'ll get the charge in writing. In the Reference code: #10214, are all files, that we found on your computer.

The sender address of this mail was masked, to protect us against mail bombs.

- You get more detailed information by the Federal Bureau of Investigation -FBI-
- Department for \"Illegal Internet Downloads\", Room 7350
- 935 Pennsylvania Avenue
- Washington, DC 20535, USA
- (202) 324-3000

Cari Alessandro e Andrea,
beh, la seconda ipotesi è quella giusta... c'è sempre in giro qualcuno che ha voglia di rompere le scatole agli altri e non ha di meglio da fare che inventarsi nuovi modi per diffondere virus.
E che dimostra quanto siamo portati a credere alle favole, purché dette bene da qualcuno di più autorevole :-(

Provate a leggere il documento a questo indirizzo: http://attivissimo.homelinux.net/security/soceng/soceng.htm e avrai conferme di quello che stiamo dicendo, che fa parte del social engineering, usato per barare.
Quanto agli antivirus: beh, raga, qui ci vuole un antivirus con le palle e soprattutto aggiornato costantemente. Se non becca un virus così, c'è da cominciare a sudare freddo...

PARLI COME BADI!

Ciao. Mi chiamo Luca e passo subito al "sodo";
ho notato che molti, come me, hanno difficoltà nello svincolarsi fra i vostri articoli. E' oltremodo frustrante impantanarsi nella lettura di un argomento che ti appassiona, perchè non conosci il significato di alcuni termini o concetti. Non si tratta altresì di parole di uso comune, facilmente reperibili su un dizionario! Ho comunque notato che ultimamente tendete a specificare sempre più anche quelle cose che per un "ossessionato" sono addirittura banali e scontate. E fate bene. Basta mettere fra parentesi un paio di parole "umane" per spiegare cose altrimenti incomprensibili. Vi consiglio di implementare sempre più questo modus operandi, poiché renderà più piacevole la lettura anche ai non espertissimi come me (oltre ad aiutarci a diventarlo!).
Vorrei lanciare un messaggio a tutti coloro i quali ritengano "palloso" leggere articoli pieni di cose per loro scontate: "nessuno è nato studiato" e quel che sapete lo sapete perchè avete avuto il tempo, la voglia e la costanza di impararlo, ma anche la fortuna di poter attingere alle fonti giuste!! Nessuno impara veramente da solo.

Luca

Ciao Luca.
Difficile dare il giusto equilibrio e accontentare tutti, vero? Ma in fondo una cosa sola ci interessa: dare lo spunto per far partire lo spirito giusto. È come quando si fa un viaggio all'estero: magari non so bene la lingua, forse non conosco le abitudini del luogo dove mi sto recando, certamente farò delle figuracce in chissà quante occasioni. E allora i casi sono due: o non parto più, o parto cogliendo tutto come un'occasione unica per aprire la mente e gli occhi, imparare cose nuove, magari anche capire che non sono solo a trovarmi in situazioni analoghe e cominciare a parlarne!
Nessuno nasce imparato, diceva Antonio de Curtis, in arte Totò (approposito, anche il titolo è suo: ma lo sapevi, vero?!). E la grande curiosità, è l'unica medicina e lo spirito del vero hacker.
Sei ancora in ascolto? E allora divertiti con http://www.antoniodecurtis.com/

MONITOR E FOTO

Quando i monitor dei PC si vedono in TV ci sono sempre delle barre che scorrono dall'alto verso il basso.
Dopo lunga meditazione ho concluso che questo effetto viene creato dalla diversa velocità di refresh dello schermo PC rispetto alla velocità dei singoli fotogrammi.
Essendo i fotogrammi + lenti del refresh del monitor non riescono a filmare l'intera sequenza ed è per questo che l'immagine risulta a scatti. Aspetto smentite. A presto

Giaipur

Caro Giaipur,
complimenti per le tue deduzioni.
È un po' quello che accade anche quando si cerca di fotografare uno schermo TV. Ma vediamo allora come si fa a fare una bella fotografia senza i problemi di barre indesiderate.
Innanzitutto disattivate il flash, non serve e darebbe un sacco di problemi. Poi impostate una sensibilità minima, diciamo 100 ASA. Mettete il tutto su cavalletto o su un altro supporto che vi permetta di centrare esattamente l'obiettivo con lo schermo.
Se vi posizionate un po' distanti e usate lo zoom, verrà ancora meglio perché si evitano le linee storte.
Meglio anche oscurare tutto, eliminare le eventuali luci e coprire i LED dei televisori. Il buio, insomma, evita di vedere strani riflessi colorati. Il tempo di esposizione deve essere uguale o più lungo del tempo di tracciamento dell'immagine sullo schermo, altrimenti verrà fuori il problema che dice il nostro Giaipur: non viene riprodotta l'immagine intera. Nel caso di un TV, un fotogramma viene disegnato in 1/25 di secondo. Se il tempo di scatto è inferiore, il risultato sarà una foto incompleta o con le bande. I migliori risultati in genere si ottengono con tempi di 1/4 o 1/8 di secondo. Con le animazioni o con i film è necessario però impostare un tempo di esposizione pari alla frequenza di refresh utilizzata. Mettete a fuoco se già non avviene automaticamente e zac! ci siete.
Un'ultima curiosità: perché adottare questa tecnica anche ai monitor PC, quando esistono i salvaschermo? Perché spesso i salvaschermo non riescono a catturare immagini provenienti in diretta (tramite streaming) dai siti 'live'. Per non trovarvi un blocco nero o violaceo, l'unica soluzione è usare la macchina fotografica.

C'È ANCORA CHI CI CREDE?

Dalla posta mi arriva regolarmente una patch, che dal mittente risulterebbe "Microsoft". Dato che uso Linux la patch non mi serve, né la voglio, ma anche le mie proteste in risposta non servono a niente. [...] Mi domando se questo messaggio sia veramente una sorta di virus della Microsoft o se sia solamente un virus mandato da chissachi.
Vi mando la pach da controllare (ovviamente non apritela senza le dovute precauzioni.... :-). Distinti saluti.

Roberto

"From: "Microsoft"
<security@microsoft.com>
To:
Dear friend , use this Internet Explorer patch now!
There are dangerous virus in the Internet now!
More than 500.000 already infected!

patch.exe"

Gentile Roberto,
hai pensato bene di non aprire la patch, ma ancora meglio avresti fatto non rispondendo a nessun messaggio del genere. Pensaci un po': ti pare che Microsoft, per quanto tu sia un accanito sostenitore di Linux, mandi in giro dei messaggi email con gli aggiornamenti del software? Semmai, come fanno tutte le grandi organizzazioni, attiva un sito da cui scaricare in modo controllato e sicuro tutto quello che potrebbe servirti. Per di più rispondere a tutte quelle email che ti dicono qualcosa come "se non vuoi ricevermi più, clicca qui", è come dire a chi ti manda spam "eccomi, esisto e sono attivo. Per favore, riempimi di spam tue e di tutti quelli a cui hai venduto (a caro prezzo) il mio indirizzo. Per di più tra quelli che valgono, perché funzionanti!"
Quindi: buttare subito tutto quello che non sapete da dove vi arrivi e del perché vi sia stato inviato. È l'unico modo per evitare pasticci. Poi attivare un buon antivirus tenuto _sempre_ aggiornato (tranquillo, il tuo file allegato è stato eliminato in modo automatico dal nostro antivirus) e usare, con parsimonia, le opzioni antispam del provider. Ecco fatto, non ci caschi più :-)

TROVAMI LA EX

Ciao ragazzi, è inutile dirvi ke siete davvero forti ;) Vi scrivo x un prob ke ho. Ho letto l'articolo sul n°40 "stringere il cerchio". Era da ytempo che cercavo degli url x trovare xsone che non sai + come e dove trovarle sul web. Ho provato tutti gli url pubblicati ma non sono riuscito a trovare la xsona ke vorrei cercare. Premetto: questa xsona è una xsona che è stata da prima la mia migliore amica e poi la mia ragazza. purtroppo ha una brutta malattia e non so se ce la farà......... io vi dgt da napoli lei è napoletana e si trasferì a rimini. Da allora non ho avuto + sue notizie. vorrei tanto rintracciarla ma non so come fare. potete aiutarmi x favoreeeeeee vorrei saxe come sta, cosa sta facendo.. insomma avete capito no?!!! se decidete di aiutarmi in questa impresa ve ne sarò grato x sempre.... mandatemi un risposta e io vi darò i suoi dati ke ho a disposizione.
grazie 1000, auguri e in culo alla balena x la vostra rivista strafica!!!

.::Momix::.

Ciao a te .::Momix::.!
Grazie dei compli, ecc ecc. Ti diciamo nell'orecchio una cosa: anche "stringere il cerchio" è nato da una esperienza più o meno come la tua! Il primo amore non si scorda mai: vero! Vabbé, ma allora come fare? Certamente cercare i privati è maledettamente difficile. E meno male. Pensa sennò quanti rompi avresti tra i c... anche tu! Però, però... se uno ci tiene sul serio si muove e non si dà pace. E allora, forse, ci riesce. Forse spendendoci qualche soldino, a volte anche no. Ti spiego. Forse non sai che i Comuni (sì, quelli col sindaco dentro...) hanno le cosiddette liste elettorali. E forse non sai che sono a disposizione di chiunque ne faccia una richiesta per uno scopo ragionevolmente credibile: chessò, offrire posto di lavoro ai diciannovenni appena diplomati. A volte chiedono qualche soldo (una ventina di Euro, al più). A volte non chiedono nulla se non di firmare un foglietto che ti spediscono .pdf, in cui si dichiara che non verranno usati per scopi illeciti. E lì trovi tutta l'anagrafica comunale dai diciott'anni in su, ovviamente senza numero di telefono. Ma non dirmi che, rileggendo l'articolo, non saresti in grado di arrivare a un numero di telefono a partire da un nome e indirizzo...
E come fare a contattare i Comuni? Niente di più semplice: www.comuni.it. Indirizza le tue richieste a Ufficio Elettorale, ma mi raccomando: non dire che ti abbiamo mandato noi! :-) E dai che la trovi!